Privacy and Security in Social Networking Sites

Swapna Singh[1], Rupal Tyagi[2], Saloni Gaur[3], Pragati Varshney[4], Daksh Gupta[5]

[1]Associate Professor, Dept. of Computer Science and Engineering, IPEC, Uttar Pradesh, India
[2-5]Student, Dept. of Computer Science and Engineering, IPEC, Uttar Pradesh, India

---***---

Abstract - *Social media such as IPEC FAMILIA is an effective and profitable way to engage students, faculties and build communities – but only if the risks are identified, mitigated, managed and monitored as part of a comprehensive social media governance plan. This site provides a pathway to a multitude of personal information. Access to such data can be great value to attackers who seek highly personalized data to carry out targeted attacks.*

Over, the last few years, social media has lifted the lid on the seedy underbelly of its platforms, which have become a new breeding ground for online scammers. This calls for advances in security protocols to safeguard against hackers which form the basis of this research. In this paper we will discuss some of the privacy and security concerns, attacks and their respective prevention techniques.

1. INTRODUCTION

Today, Social networking platforms are moved from early adoption phase to organization level adoption and are emerging as next generation vehicles. Social networking platforms create and cultivate focused communities/networks to facilitate communication at all levels. There is a shift from document-centric to people centric networking. Everything is becoming social so are we.

Ipec Familia is a platform where staff members and students can come together to bridge the communication gap. It provides a platform where anyone can create their profile, post, share stories, follow other members available on the site, send messages to them, discussion forum is provided that gives the availability of study material, people's suggestion to be available at one place.

But however, the social media platforms that we use a hundred times a day to keep up with friends, family and updates have given rise to a vast global cybercriminal network. IPEC FAMILIA provides a pathway to a multitude of personal information. Access to such data can be of great value to attackers who seek highly personalized data to carry out targeted attacks like spear-phishing or compromise business email systems that can happen anywhere including our own college premises. With users choosing to access social media on mobile platforms, consumers such as the students and faculties need to be extra vigilant in the face of increasing sophisticated attacks on endpoint devices.

The reason why cyber-conspirators prey on these networks is because users upload their personal information that commonly include their interests, social relationships, pictures, confidential information and other media content, and share this information to the whole world via social networking sites which are very easily accessible. Faculties too, unknowingly share plethora of personal information on social networking site thus putting their corporate infrastructure and data at a risk. The volume and ease of accessibility of personal information available on these sites have attracted malicious people who seek to exploit this information. Due to the sensitivity of information stored within social networking sites, intensive research in the area of information security has become an area of paramount importance.

Privacy Options	Facebook	Twitter	Linked In	Google+	Ipec Familia
Restrict the visibility of theactive users	Yes	No	No	No	Yes
Set the control on how others can find you	Yes	Yes	Yes	No	No
Block the users for their photo tag	Yes	No	No	Yes	No
Set login alerts	Yes	No	No	Yes	Yes
Block spam users	Yes	Yes	Yes	Yes	Yes
Control who can message you	Yes	No	Yes	Yes	Yes

1.1. Privacy and Security in Accordance with Ipec Familia (college social networking site)

In the Table above, we had identified the different privacy mechanisms that the social media site offered to the users to set in and engage in the privacy concerned activities. There would be a wide range of discrimination persists in the social media sets in offering the privacy policies to the users and from the survey taken, it has largely been noted that many of the users of social media sites have not concern more on their privacy settings and kept the privacy details as such created.

2. GOVERNMENT NINE PRINCIPLES ON PRIVACY

In October 2012 the Report of the Group of Experts on privacy was published by a committee of experts chaired by Justice A.P. Shah[7][11].The report creates a set of recommendations for a privacy framework and legislation in India. Most importantly, the Report recognizes privacy as a fundamental right and defines nine National Privacy Principles that would apply to all data controllers both in the private sector and the public sector. This would work to ensure that businesses and governments are held accountable to protecting privacy and that legislation and practices found across sectors, states/governments, organizations, and governmental bodies are harmonized.

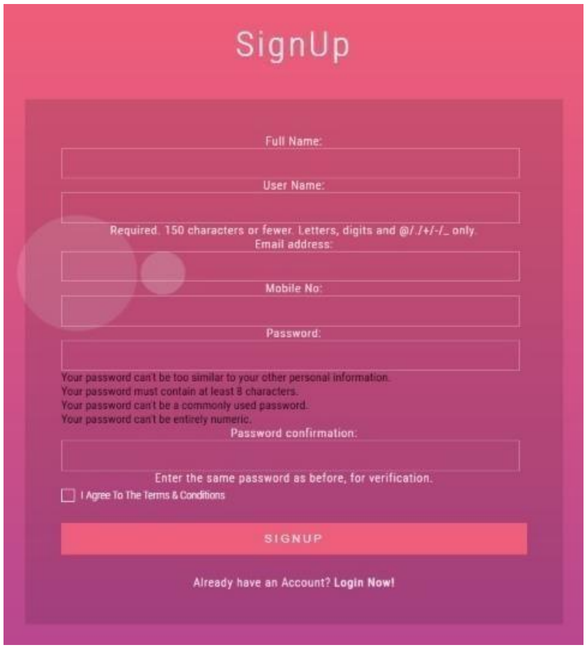
The nine national privacy principles include:

2.1. Principle 1 - Notice

A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include:

During Collection – these are the security guidelines every social media must follow:

- What personal information is being collected;
- Purposes for which personal information is being collected;
- Uses of collected personal information;
- Whether or not personal information may be disclosed to third persons;
- Security safeguards established by the data controller in relation to the personal information;
- Processes available to data subjects to access and correct their own personal information;
- Contact details of the privacy officers and SRO ombudsmen for filing complaints.



SignUp

Full Name:

User Name:

Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Email address:

Mobile No:

Password:

Your password can't be too similar to your other personal information.
Your password must contain at least 8 characters.
Your password can't be a commonly used password.
Your password can't be entirely numeric.

Password confirmation:

Enter the same password as before, for verification.

□ I Agree To The Terms & Conditions

2.2. Principle 2 - Choice and Consent

A data controller shall give individuals choices (opt- in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a reasonable timeframeif published in public databases.

2.3. Principle 3 - Collection Limitation

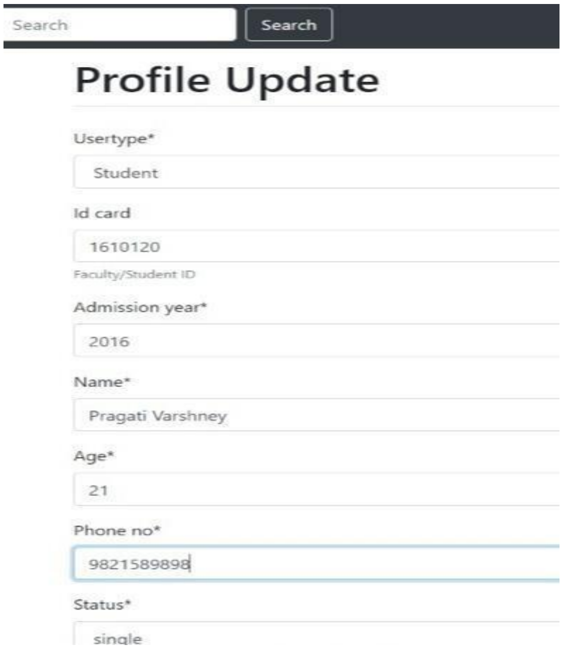
A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

2.4. Principle 4 - Purpose Limitation

Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.

2.5. Principle 5 - Access and Correction

Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.



Profile Update

Usertype*
Student

Id card
1610120
Faculty/Student ID

Admission year*
2016

Name*
Pragati Varshney

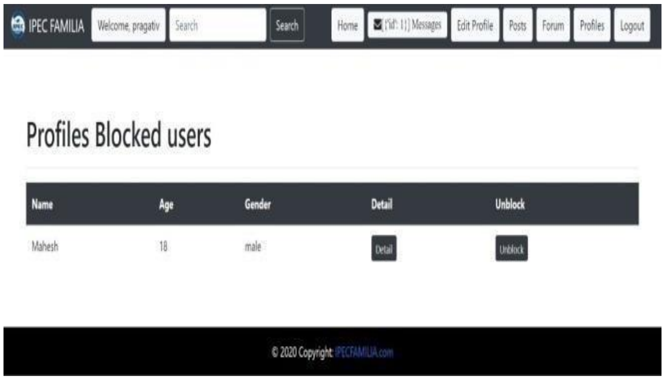
Age*
21

Phone no*
9821589898

Status*
single

2.6. Principle 6 - Disclosure of Information

A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.



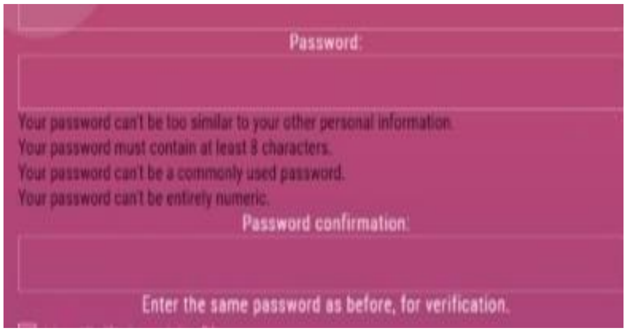
Profiles Blocked users

Name	Age	Gender	Detail	Unblock
Mahesh	18	male	Detail	Unblock

© 2020 Copyright: IPECFAMILIA.com

2.7. Principle 7 - Security

A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorized access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.


Password:

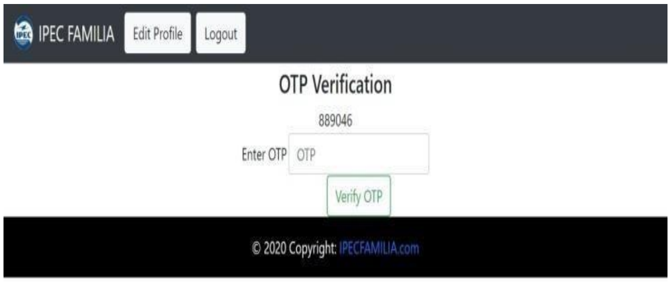
Your password can't be too similar to your other personal information.
Your password must contain at least 8 characters.
Your password can't be a commonly used password.
Your password can't be entirely numeric.

Password confirmation:

Enter the same password as before, for verification.

2.8. Principle 8 - Openness

A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.



OTP Verification

889046

Enter OTP: OTP

© 2020 Copyright: IPECFAMILIA.com

In IPECFAMILIA, we use two factor authentications: knowledge factor and possession factor.

The knowledge factor is something that the user knows, such as a password, a PIN, or some other type of shared secret. The possession factor is something that user has, such as an ID Card, a security token, a cellphone, a mobile device or a smartphone app, to approve authentication requests.

2.9. Principle 9 - Accountability

The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

3. Protecting Information Security and Privacy on Social Media:

The best way of dealing with menace of cybercrimes emanating from social media is to make users aware of information security and privacy issues. The users also need to understand how to use the social media platforms responsibly.

Some of the best practices while using social media are:

1. **Remove Unnecessary Personal Information:**

   Don't reveal personal information, date of birth, photos, mother's maiden name, etc.

2. **Adjust Privacy and Security Settings:** Configure the application's security and privacy settings and make best use of all available security features.

3. **Do not accept friend requests from strangers:** Reject all friend's requests from strangers as criminals may also easy access to your profile and information.

4. **Use strong password:**

   Always use strong, lengthy and unique passwords for all social media accounts. This will make the passwords compromise more difficult.

5. **Protect your password:**

   Do not share your social media passwords even with your best friends. Where ever possible use multi factor authentication for the accounts.

6. **Remove Installed Third-Party Applications:** Third party applications access lot of personal information of the users and may also share or sell that information to others.

7. **Do Not Publish Your Location:**

   Avoid using geotagging while using social media like the 'check-in' feature in Facebook app as cybercriminals might misuse this information.

8. **Do not trust your online social network friends:**

   There are lot of fake users on the social media, so do not share any information with such 'friends' unless their authenticity is properly verified.

9. **Monitor your children's online social network activities:**

   Children become easy prey to online predators hence always monitor their activities on social networking sites.

10. **Always think twice before posting something:**

    Do not post anything on social media unless you are very sure that the post will not compromise your data security or privacy. Also, always remember that the content in your post is not going to offend anyone.

11. **Always update your software:**

    There is nothing like 100 percent secure application and the vendors regularly send updates to the users which tries to mitigate vulnerabilities discovered. Also, apart from applications the users should always update the operating system software (like Android, iOS, etc.)

12. **Always use good internet security / antivirus software:**

    A good Internet security / antivirus software will enhance the security by preventing compromise of sensitive data of the user on the device. Always the user should update the antivirus software on regular basis.

13. **Follow ethics:**

    While using Internet and social media users should follow ethics such as hiding personal information, avoiding bad language, avoid sharing and downloading copyrighted material without proper permission, pretending to be someone else or identity spoofing, spamming, respecting other cultures and religions, trolling others, etc.

4. SUGGESTION

We would like to suggest few simple ways to stay safe while using social media:

- Use a password manager: Do not use either the exact same password or a variation of the same password for multiple accounts. Password manager remember all of your passwords for you, storing them in an encrypted vault. You'll only have to remember one master password, which you can use to log on to all of your social media accounts. You can even set up two-factor authentication.

- Read Privacy Policies: everyone must carefully read the privacy policy of social networking site in which they are registering themselves so that they come to know the way the company uses their data and agree to that only if they are okay with it.

- Customize Privacy Settings: Customize your privacy settings to control who can and can't see your content.

- Log Off when Done: It is easy to leave yourself logged in on all the apps on your phone, especially because we use them so often. But if you lose your phone, or any mobile device, and you're still logged into social media accounts, then you're making it very easy for hackers to access your accounts and steal your personal information. Even though it may seem like a hassle, be sure to log out of social media accounts when you're done using them.

- Lock Phone: make sure that your phone locks automatically after a certain period of time maximum 30 seconds. On top of that, make a passcode that's as long as possible and not based on anything obvious.

- Use a VPN (Virtual Private Network): VPNs encrypt your web traffic in a tunnel, replacing your IP address so that hackers won't be able to access any of your information.

- Use of Session Time out: A 30minute session timeout has been given to IPECFAMILIA.

5. CONCLUSION

Social networking sites are both boon and bane for our society and individuals. On one hand **Social media** has facilitated a lot in reshaping communication industry and redefining the ways in which we communicate and express ourselves. But on the other side it has major problems with respect to privacy of information and security. Due to enormous database of users and their sensitive and personal information, social media has become a potential target of many cybercriminals.

Through our research we can conclude that up to some extent our privacy and security lies in our hand only as when we create new id in any social media platforms and register ourselves then we come across to their terms and conditions including privacy policy, which we must read carefully and then agree to those conditions because in those terms and conditions we come across how are data will be used and up to what extended. But due to lack of privacy and security awareness in society most people do not care about their data or privacy on social media as they are unaware of the threats and risk they take while making their data freely available on social media and falling prey to attackers. Major concern nowadays is that people are in some cases unaware of privacy and security so we feel that more programs to be conducted in educating the societies the way to use social media in right way and securely and make them aware of the privacy and security option available in each and every social networking sites under settings options, so they can control their data efficiently at their level and decrease their risks for attacks. Secondly, we think social networking sites must safeguard privacy and security of its users at all levels. The Report of the Group of Experts on Privacy and the government considering a draft privacy bill are all steps in the right direction. The revised Personal Data Protection Bill, 2019(Draft Bill), which was cleared by the Union Cabinet is a step in right direction, and will increase awareness and vigilance against data breaches.

REFERENCES

1. https://www.statista.com/statistics/27 8407/number-of-social-network- users-in-india/

2. https://www.statista.com/statistics/28 4436/india-social-network- penetration/

3. https://www.statista.com/statistics/30 4827/number-of-facebook-users-in- india/

4. https://www.statista.com/statistics/26 8136/top-15-countries-based-on- number-of-facebook-users/

5. https://www.statista.com/statistics/73 7411/ipl-teams-with-the-highest- facebook-likes-india/ https://www.statista.com/statistics/717615/india-number-of-facebook- users-by-age-and-gender/

6. https://cis- india.org/telecom/knowledge-repository-on-internet- access/internet-privacy-in-india

7. http://www.zdnet.com/in/india-sets- up-social-media-monitoring-lab- 7000012758/

8. http://www.techdirt.com/articles/201 30203/18510621869/investigative- journalist-claims-her-public-tweets- arent-publishable-threatens-to-sue- blogger-who-does-exactly-that.shtml

9. http://www.npr.org/blogs/alltechcons

idered/2013/10/02/228134269/your- digital-trail-does-the-fourth- amendment-protect-us

10. Report of the Group of Experts on PrivacyAvailable at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

11. https://www.trp.org.in/wp-content/uploads/2017/08/AJMS- Vol.6-No.2- July-December-2017- pp.42-49.pdf

12. NIST Special Publication PII 800- 122.Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 122.pdf

13. Handbook on European Data Protection Law. Retrieved from Handbook on European data protection law EU-2014-handbook- data- protection-law-2nd-ed_en.pdf